



HEALTH AFFAIRS



HIPAA Privacy Essentials

HIPAA Training

TMA Privacy Office

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

Training Objectives

- Once you have completed this course you should be able to:
 - Provide an Overview of the HIPAA Privacy Rule
 - Identify the Core Concepts of the HIPAA Privacy Rule

HIPAA Privacy Rule Overview

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

HIPAA Privacy Rule Overview

Objectives

- Upon completion of this module, you should be able to:
 - Explain the background of HIPAA and the HIPAA Privacy Rule
 - Identify how HIPAA privacy fits in to the HIPAA Law
 - Explain the relationship of the HIPAA Privacy Rule to other Laws
 - Describe the purpose and applicability of the HIPAA Privacy Rule
 - Explain the structure of the HIPAA Privacy Rule

HIPAA Privacy Rule Overview

HIPAA

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191 was designed to:
 - Improve portability and continuity of health insurance coverage
 - Improve access to long term care services and coverage
 - Simplify the administration of health care

HIPAA Privacy Rule Overview

HIPAA Legislation

- HIPAA under PL 104-191 requires compliance with several standards, including:
 - Standards for Electronic Transactions and Code Sets
 - Privacy
 - Security Standards
 - Electronic Signature Standards
 - National Standard Employer Identifier
 - National Standard Health Care Provider Identifier
 - National Standard Health Plan Identifier

HIPAA Privacy Rule Overview

Components of the Privacy Rule

Privacy Rule ensures:

- Rights for the individual patient
- Boundaries on use and release of protected health information
- Security of protected health information
- Accountability and penalties
- Balance of public responsibility with protections
- Preservation of stronger state laws

HIPAA Privacy Rule Overview

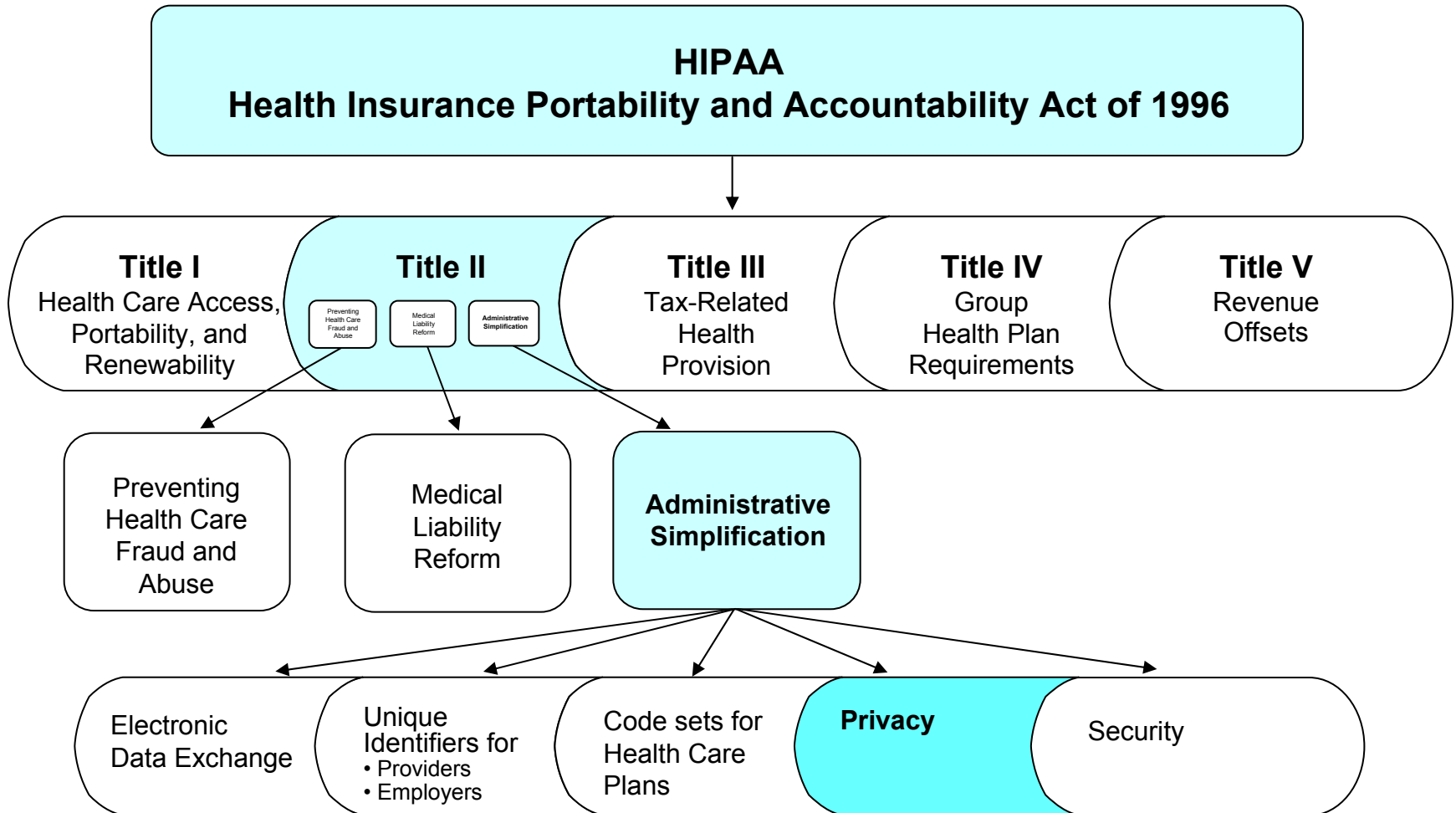
In a Nutshell



- Initial rule stated that a covered entity may not use or disclose protected health information (PHI) unless:
 - the patient agrees to the use or disclosure, or
 - the use or disclosure is specifically required or permitted by the HIPAA regulations
- In March 2002, HHS proposed changes that included elimination of the requirement for patient consent for this purpose. Under the proposal:
 - A covered entity need only notify patients about their rights and the entity's practices
 - Consent for uses and disclosures applies only to treatment, payment and health care operations (TPO)
 - Authorizations are still required for use & disclosure of information for non-TPO purposes

HIPAA Privacy Rule Overview

Where Does This Fit In?



Source: National Institute of Standards and Technology (NIST)

HIPAA Privacy Rule Overview

Relationship to Other Law (1 of 2)

- HIPAA does not preempt or cancel existing federal law
 - Privacy Act
 - DoD's implementation of HIPAA Privacy and Privacy Act do not conflict
 - Compliance with Privacy Act does not ensure compliance with HIPAA and vice versa
 - The covered entity must comply with HIPAA and Privacy Act
 - Alcohol and Drug Abuse, and Mental Health Administration Reorganization Act
 - The covered entity must comply with HIPAA and Privacy Act
 - Always follow the more restrictive rule

Relationship to Other Law (2 of 2)

- With regard to state law, follow whichever is more restrictive except:
 - Follow state law with regard to disclosure of PHI about minors to those legally responsible for the minor





HIPAA Privacy Rule Overview

Purpose of the HIPAA Privacy Rule

- The HIPAA Privacy Rule is designed to protect the privacy of individually identifiable health information by:
 - Dictating how covered entities may use and disclose an individual's health information
 - Establishing patient rights with regard to their health related information

HIPAA Privacy Rule Overview

Applicability of the HIPAA Privacy Rule

<u>HIPAA ENTITY</u>		<u>MHS ENTITY</u>
Providers who use a covered transaction		MTFs, DTFs and clinics
Health plans		TRICARE Health Plan
Healthcare clearinghouses		Companies that perform electronic billing on behalf of MTFs
Business associates		Managed care support contractors and other contractors

HIPAA Privacy Rule Overview

Applicability

- HIPAA Privacy Rule applies to all DoD health plans and DoD providers
- Does not apply to:
 - Drug abuse testing programs
 - Armed Forces Repository of Specimen Samples for the Identification of Remains
 - Military Entrance Processing Stations
 - Education and day care centers
 - Provision of care to foreign nationals occurring outside of the United States

HIPAA Privacy Rule Overview

Rule Structure (1 of 2)

- §164.502 general rules contains 10 standards that provide the high level requirements
- Each of the 10 standards then refers to other sections for specifics
- Those standards are:
 - No use or disclosure except as permitted or required
 - Minimum necessary requirements
 - Uses and disclosures subject to agreed upon restriction
 - De-identification of PHI
 - Disclosures to business associates

HIPAA Privacy Rule Overview

Rule Structure (2 of 2)

- Deceased individuals
- Personal representatives
- Confidential communications
- Notice of Privacy Practices
- Disclosures by whistleblowers and workforce member crime victims

HIPAA Privacy Rule Overview

Summary

- You should now be able to:
 - Explain the background of HIPAA and the HIPAA Privacy Rule
 - Identify how HIPAA privacy fits in to the HIPAA Law
 - Explain the relationship of the HIPAA Privacy Rule to other Laws
 - Describe the purpose and applicability of the HIPAA Privacy Rule
 - Explain the structure of the HIPAA Privacy Rule

Core Concepts

Core Concepts

Objectives

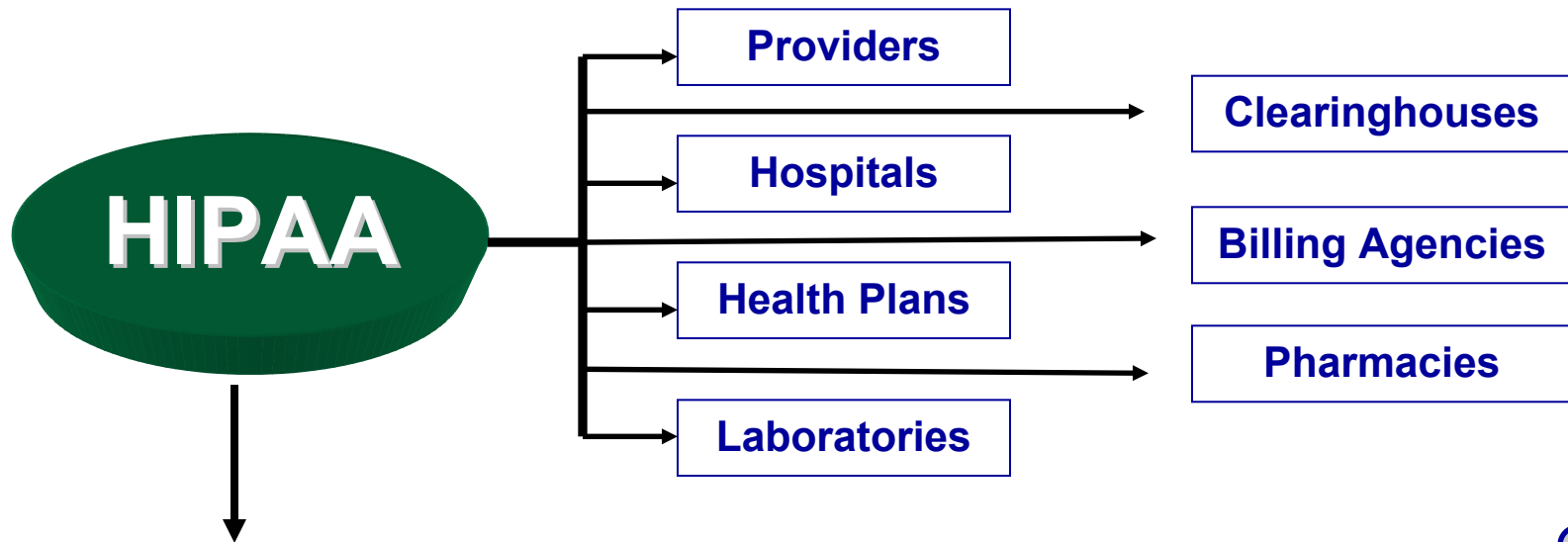
- Upon completion of this module, you should be able to:
 - Describe a Covered Entity and the requirements for a CE
 - Identify various types of Health Information
 - Explain Treatment, Payment, and Healthcare Operations under the HIPAA Privacy Rule
 - Describe Workforce and requirements according to HIPAA
 - Outline Patient Rights
 - Define the Minimum Necessary Principle
 - Describe the Roles and Responsibilities of a Privacy Officer

Covered Entity

- Covered entities are health care providers who transmit health information in (standard) electronic transactions
- Covered entities fall into four categories:
 - Health plans
 - Health care clearinghouses
 - Health care providers
 - Business associate relationships

Core Concepts

Covered Entities



Indirect Applicability: All organizations that exchange data with those directly covered under the HIPAA through Business Associate Agreements and/or contracts

Organized Health Care Arrangement

- HIPAA allows each of the CE's in the OHCA (TRICARE) to use the policies and procedures and the Notice of Privacy Practices established by the OHCA as their own
- Includes:
 - MHS
 - Army
 - Navy
 - Air Force
 - Coast Guard

Safeguards and Sanctions

- HIPAA requires you to protect the privacy of PHI using appropriate and reasonable administrative, physical and technical safeguards
- Safeguards should:
 - Enforce HIPAA Privacy requirements
 - Limit incidental use and disclosure of PHI
- Develop and implement an appropriate sanction policy
- In addition to administrative safeguards and other actions, sanctions may include:
 - For members of the military: action under the Uniform Code of Military Justice
 - For civilians: sanctions consistent with Chapter 75 of Title 5, USC
 - For contractors: actions permissible under procurement regulations

Core Concepts

Mitigation

- At each covered entity, you must take positive action to minimize known harmful effects resulting from the unauthorized use or disclosure of protected health information, and are obligated to correct known instances of harm
- Business associates have an obligation to notify the covered entity of any harmful effect they know about
- Enterprise-wide shared aggregate databases are potential problems

Mitigation Policies

- Contain the damage and stop further compromise
- Inform those responsible for the breach to prevent future harmful actions
- Consider whether appropriate to notify patient
- Include contract language to transfer the potential financial burden of harm to business associates

Documentation

- Document privacy policies and procedures in written or electronic form
- Document required communications, designations, actions and activities
- Record date of creation and last date of effectiveness of documents
- Maintain required documentation for six years from date of creation or the date when the policy or procedures was last in effect, whichever is later
- Make documentation available
- Clearly delineate title/office and assigned responsibilities

Health Information

- Health Information (HI) is any information, whether oral or recorded in any form or medium, that:
 - Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual

Core Concepts

IIHI / PHI / EPHI



- Individually Identifiable Health Information (IIHI) is a subset of health information, including demographic information, collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse
- PHI is a specific type of health information collected from an individual that is created or received by a health provider, health plan, or employer that meets certain criteria
- EPHI is PHI in electronic form that is transmitted or maintained by electronic media

Identifiers (1 of 2)

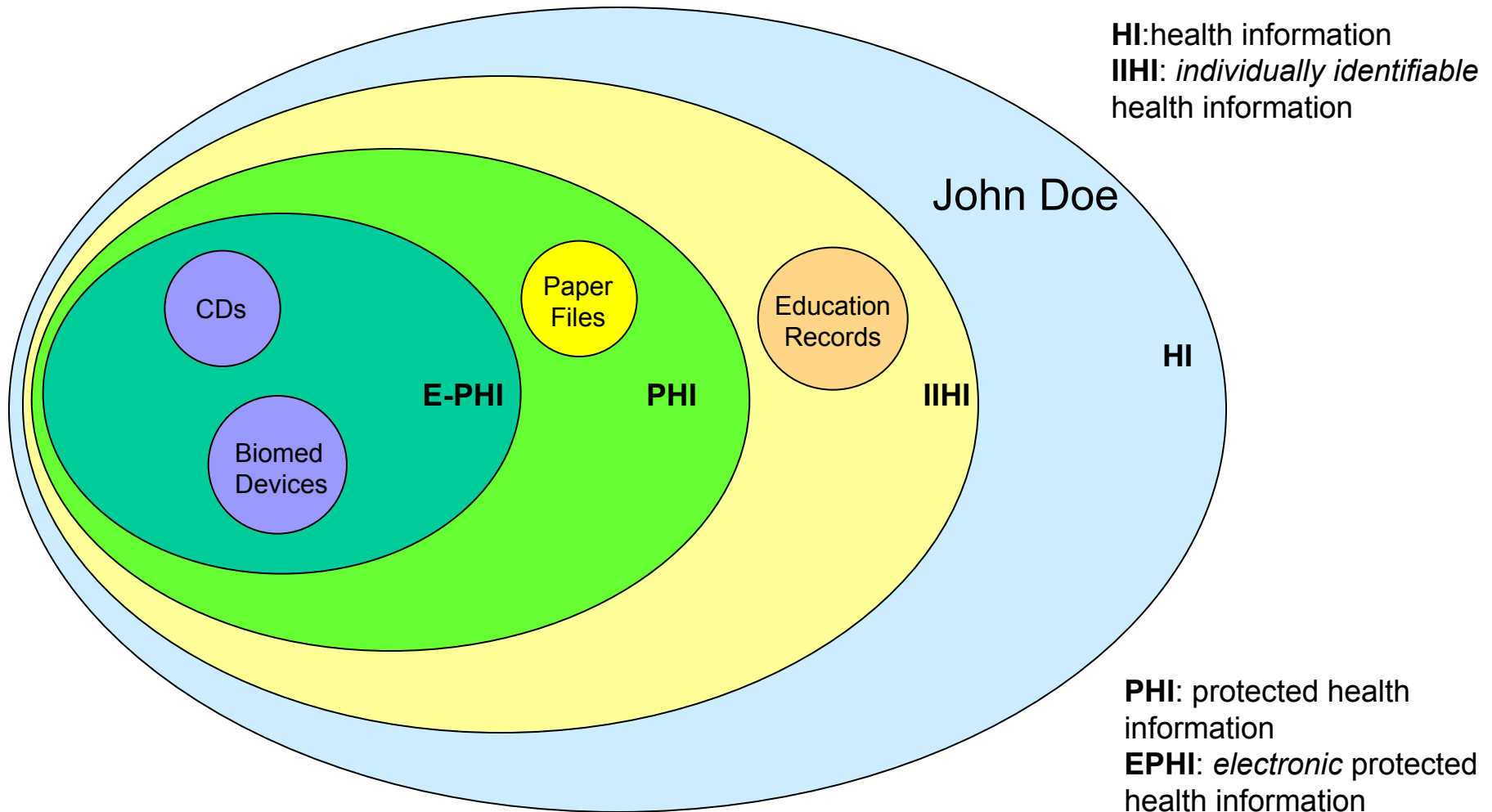
- The listed identifiers are:
 - Names
 - Geographic subdivisions smaller than a state (e.g. street address, city, county, precinct, zip code)
 - All dates (except year) (e.g. birth date, admission date, date of death etc.)
 - All dates and numbers (including year) that indicate a persons age if over 89
 - Telephone and fax numbers
 - Email address
 - Social security numbers
 - Medical record numbers
 - Health plan beneficiary numbers
 - Account numbers
 - Certificate or license numbers
 - URLs

Identifiers (2 of 2)

- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic except an assigned code that meets HIPAA requirements
- Codes assigned to aide in re-identification may not use information related to individual or allow a person to identify the individual
- You must not use or disclose code for any other purpose
- You must not disclose the re-identification mechanism

Core Concepts

The Universe of Health Information



Core Concepts

Activity

- Fax print out of a patient referral for an appointment
- Your medical history on your PDA
- School immunization records
- Digital phone message of appointment reminder
- Printed receipt for payment of medical services
- Diagnosis contained an MRI
- Printed patient medical history

PHI	EPHI	Neither

Core Concepts

Activity

- Electronic college transcript
- Lab results discussed over the telephone with a doctor
- Social Security Number
- Pathology results saved to CD
- Username and password
- A patient's name and health status emailed by family
- Employee dental billing information on a laptop

PHI	EPHI	Neither

De-identified Health Information

- You may use PHI to create de-identified health information
 - De-identified information cannot be traced back to a specific individual
- De-identified health information is not subject to regulation
- Two methods to verify de-identification of information
 - Expert in statistical analysis and de-identification of information must analyze the information and attest that it does not contain elements that would identify an individual or aide in the identification of an individual when combined with other available data. The method of analysis and results must be documented
 - Remove the listed identifiers associated with the individual, relatives, employers or household members and any other information that might identify the individual

Treatment, Payment and Healthcare Operations (TPO) (1 of 2)

- Treatment is the provision, coordination, or management of healthcare and related services by one or more healthcare providers
- Payment is those activities undertaken by health plans and providers to obtain premiums or provide reimbursement for services
- Healthcare operations are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment

Treatment, Payment and Healthcare Operations (TPO) (2 of 2)

- HIPAA allows the use and disclosure of PHI for treatment, payment & healthcare operations (TPO) without the patient's permission
- HIPAA Privacy is not meant to impede the provision of quality care

Core Concepts

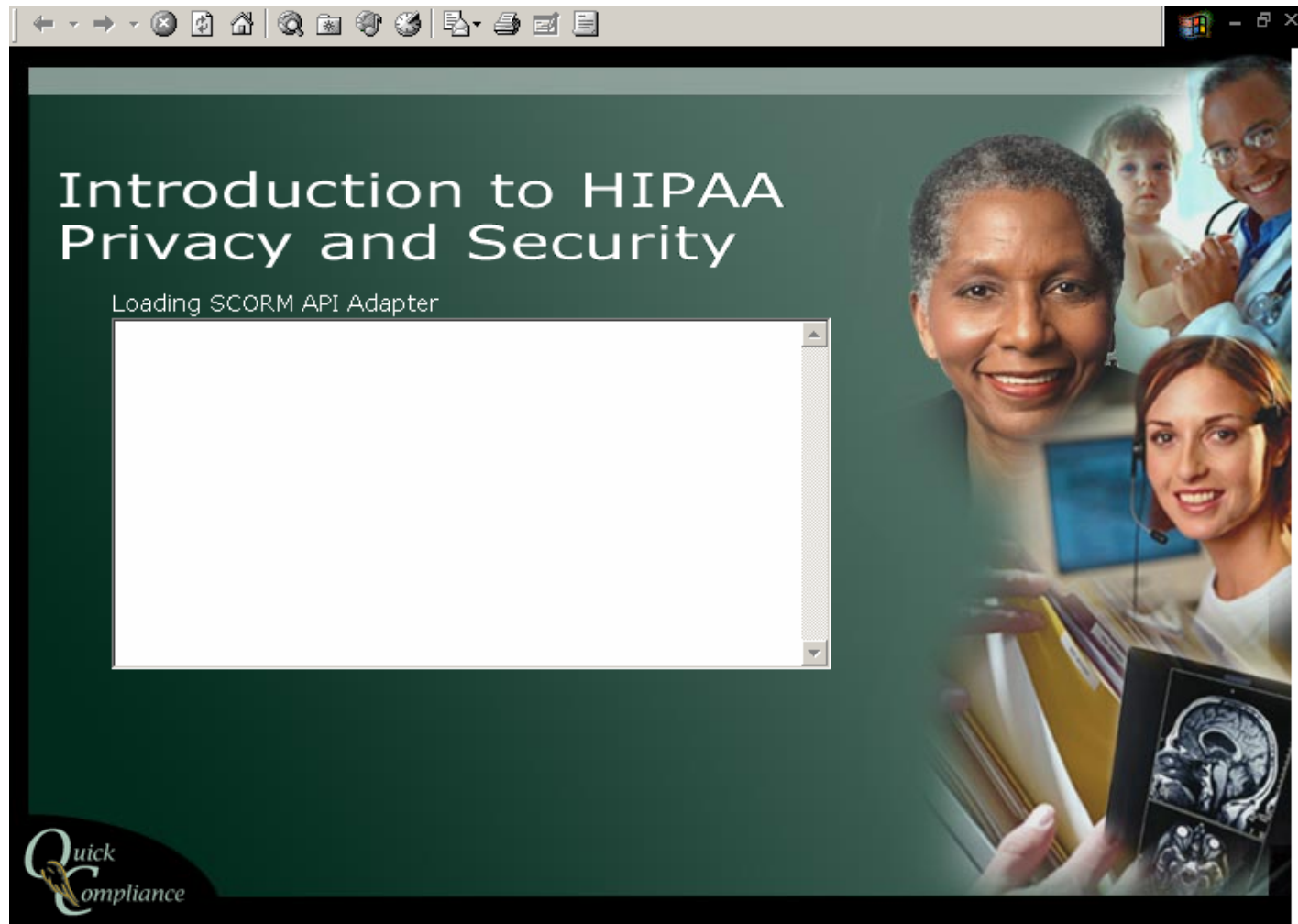
Workforce Training

- Privacy and security awareness training must be delivered to
 - Entire workforce by compliance date
 - New employees following hire
 - Affected employees after material changes in policies
- Training should discuss penalties related to non-compliance
- For compliance, document training




Core Concepts


HIPAA Training



HIPAA Refresher Training

HIPAA 210: The HIPAA Privacy Refresher

 Click a lesson name to go to the lesson

 Transforming Knowledge into Practice [Disclaimer](#)

Patient Rights

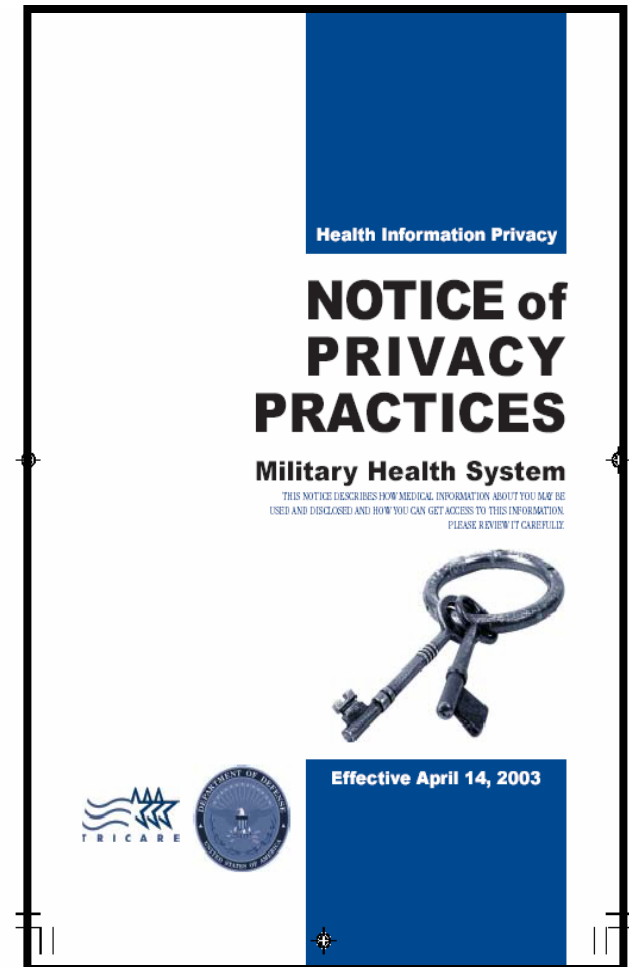
- Patients have a right to:
 - Receive a written Notice of Privacy Practices (NOPP)
 - Request access to PHI
 - Request amendment of PHI
 - An accounting of disclosures of PHI
 - Request confidential communications
 - Request restrictions on uses and disclosures
 - Complain to the MTF, TMA or DHHS



Core Concepts

Notice of Privacy Practices (NOPP)

- Explains:
 - MHS duty to protect health information
 - How the MHS may use and disclose PHI
 - Patients' rights
 - Patient complaint procedures
 - Contact information



Notice Contents (1 of 2)

- NOPP explains that MHS may use or disclose PHI:
 - For Treatment, Payment and Health Care Operations
 - When required by law or for legal proceedings
 - For law enforcement purposes
 - To public health authorities
 - For health oversight
 - To the FDA
 - To coroners, funeral directors
 - For organ donations
 - For research

Notice Contents (2 of 2)

- For military activity and national security
 - To comply with worker's compensation laws
 - To correctional facilities regarding inmates
 - By the health plan
 - To parents or guardians
- NOPP explains that MHS may use or disclose PHI unless they object:
 - In MTF directories
 - To individuals involved in their health care

Acknowledging the Notice

The signature below only acknowledges receipt of the Military Health System Notice of Privacy Practices, effective date 14 April 2003.

Name of Patient/Representative	relationship to patient (if applicable)
--------------------------------	---

☐ Patient/Representative declined to sign _____ MTF staff initials

Core Concepts

Right of Access (1 of 2)

- Individuals may request access to, or copies of, their PHI, including:
 - Medical records
 - Billing records
 - Other records used in making decision concerning the individual
- Does not include the right of access to:
 - Psychotherapy notes
 - Information compiled in anticipation of, or use in, a civil, criminal or administrative action or proceeding
 - PHI that is subject to law that prohibits access

Right of Access (2 of 2)

- Patient request for access to PHI must be in writing
- You must grant or deny request within:
 - 30 days for records you possess
 - 60 days for PHI maintained or accessible only at another site
- You may extend time by no more than 30 days if you provide the individual with written
 - Explanation as to why there is a delay
 - Date for final action

Core Concepts

Granting Access

- Notify individual and provide access or copies within required time period
- If PHI is duplicated at more than one location you only have to provide it once
- Provide the PHI in requested format if reasonable
 - If not, provide in readable hardcopy or other agreed upon format
- Provide summary or explanation of PHI only when the individual agrees in advance
- You may impose a reasonable cost based fee for supplies and labor in accordance with service policy
 - You must inform the individual of those fees in advance

Denial of Access (1 of 5)

- The CE may deny the request without the opportunity for review when the PHI is
 - Psychotherapy notes
 - Compiled for use in a civil, criminal or administrative action or proceeding
 - A disclosure prohibited under the Clinical Laboratory Improvements Amendments of 1988
 - A disclosure prohibited under the Title 10, USC, Section 1102, Confidentiality of medical quality assurance records
 - To an inmate in correctional institution, if access would jeopardize the health, safety, security, custody or rehabilitation of the individual, other inmates, or any officer employee or other person at the facility

Denial of Access (2 of 5)

- Access may be denied if the
 - Individual is participating in a research project and they have signed a consent clause suspending right of access
 - Only while the research is in progress
 - PHI was obtained from someone other than a provider under promise of confidentiality and providing access could reveal the source
- If access is denied, the individual may request a review for following reasons:
 - Licensed health care professional determined granting access will endanger life or physical safety of individual or other person

Denial of Access (3 of 5)

- If PHI references someone other than the individual or provider and access may cause substantial harm to that person
- Request is made by personal representative of the individual and granting access could cause substantial harm to the individual or another person
- Review must be by a licensed health care professional designated to act as a reviewing official but who did not participate in the original decision to deny
- Note: Access to most PHI is also subject to the Privacy Act. You must grant access to PHI unless access can be denied under the DoD implementing policies for **both** laws.

Denial of Access (4 of 5)

- Denials must be written in plain language and contain:
 - Basis for the denial
 - A description of how the individual may exercise their right to a review
 - How the individual may file a complaint to both the DoD and the Secretary of HHS
- If individual requests a review you must:
 - Provide review by licensed health care official not involved in initial denial
 - Provide review in reasonable period of time
 - Notify individual of result in writing

Denial of Access (5 of 5)

- If denial pertains to only part of the request you must provide access to any other requested PHI
- You must inform an individual where to direct a request for PHI that you do not maintain if you know where it is located

Right to Request an Amendment

- Individuals have the right to request that you amend the PHI you maintain
- You must grant or deny the request within 60 days
 - You may extend the time period only once for no more than 30 days if you inform the individual in writing and include the reason for the delay and date they can expect a decision

Granting an Amendment

- If you agree to make the amendment:
 - Notify the individual in writing
 - Make reasonable effort to notify other persons the individual identifies and agrees should know of the amendment
 - Provide the amendment to other people, including business associates, who possess the PHI and may use it to the individual's detriment
 - You may amend the PHI by identifying the records that are affected and appending or providing a link to the amendment

Denying an Amendment (1 of 4)

- You may deny a request for an amendment for the following reasons:
 - You did not create the PHI, unless the individual provides reason to believe the originator of the information is no longer available
 - The affected PHI is not part of the designated record set
 - The individual does not have a right of access to the affected PHI
 - The PHI is accurate and complete

Denying an Amendment (2 of 4)

- When denying the request (in whole or in part) you must provide individual with a denial written in plain English that contains:
 - Basis for the denial
 - Description of how the individual may submit a written statement of disagreement including the basis for disagreement
 - How the individual may file a complaint to both the TMA Privacy Office and the Secretary of HHS
 - Individuals right to request that you include the original request for amendment and the denial with any future disclosures of the affected PHI

Denying an Amendment (3 of 4)

- You may limit a statement of disagreement to a reasonable length and create an accurate summary of the statement for inclusion with disclosures
- You may prepare a written rebuttal for inclusion if you provide the individual with a copy
- You must identify the disputed PHI and append or otherwise link the individual's request for amendment, the denial, the statement of disagreement, if any, and the rebuttal, if any to the record
- You must include the above documentation with all future disclosures of the disputed PHI

Denying an Amendment (4 of 4)

- When making future disclosure using a standard transaction you may transmit the material separately
- You must amend the affected record when you receive an amendment to an individual's PHI from another covered entity

Accounting of Disclosures

- Individual may request an accounting of all disclosures (including to or by business associates) during the previous six years except for disclosures:
 - For TPO
 - To the individual themselves
 - That are in response to an authorization
 - For the facility's directory
 - To persons involved in the individual's care
 - For authorized national security or intelligence purposes
 - To correctional institutions or law enforcement officials as authorized
 - Occurring before April 14, 2003

Confidential Communications

- Individuals have the right to request receiving communications from you by alternate means or at alternate locations
- You must agree to such requests when reasonable
- You may require the request in writing with details of specific alternatives
- You cannot require the individual to explain the basis for their request

Core Concepts

Restricting Uses and Disclosures

- Individual's have the right to ask you to restrict uses and disclosures of PHI for TPO and for involvement in their care
- You may grant or refuse the request
- If you grant the request you must abide by the agreement except in emergencies
- Requests may be made in writing or orally
- No agreement to restrict applies to levels of management higher than that agreeing to the restriction
- You should respond to a request as soon as practicable and include reasons for a denial
- You may terminate a restriction upon written notice to the individual or the written or oral request of the individual

Core Concepts

Complaints

- Individuals have the right to make a complaint concerning your or TMAs implementation and compliance with the rule
- You must provide a complaint process and make it available to all patients
- You must document all complaints and their disposition
- You must not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising their rights or obligations established by the rule or DoD's implementing regulation

Patient Inquiry and Complaint Process

- DoD Regulation outlines guidelines for patient inquiry and complaint processes
 - If possible, build into existing patient inquiry and complaint procedures
- MTF designated HIPAA Privacy Officer is central point of contact
- Managed care support contractors will route issues through lead agents
- Document decisions and notify patient

Minimum Necessary Principle

- All uses and disclosures of information are limited by the 'need-to-know' standard
- Only the amount of information reasonably necessary to achieve the purpose of the release is permitted

Privacy Officer Rules & Responsibilities

- Each DoD covered entity must appoint in writing a privacy official responsible for developing and implementing its privacy policies and procedures
 - Oversee activities related to compliance with the HIPAA Privacy Rule and related Security components
 - Establish procedures to track access, use and disclosure of PHI
 - Ensure adherence to MHS policies and procedures at MTF level
 - Training the workforce in local policies and procedures
 - Monitor business associate agreements related to privacy concerns
 - Investigate patient complaints regarding privacy infractions

Core Concepts

Summary

- You should now be able to:
 - Describe a Covered Entity and the requirements for a CE
 - Identify various types of Health Information
 - Explain Treatment, Payment, and Healthcare Operations under the HIPAA Privacy Rule
 - Describe Workforce and requirements according to HIPAA
 - Outline Patient Rights
 - Define the Minimum Necessary Principle
 - Describe the Roles and Responsibilities of a Privacy Officer

Training Summary

- You should now be able to:
 - Provide an overview of the HIPAA Privacy Rule
 - Identify the Core Concepts of the HIPAA Privacy Rule

Resources

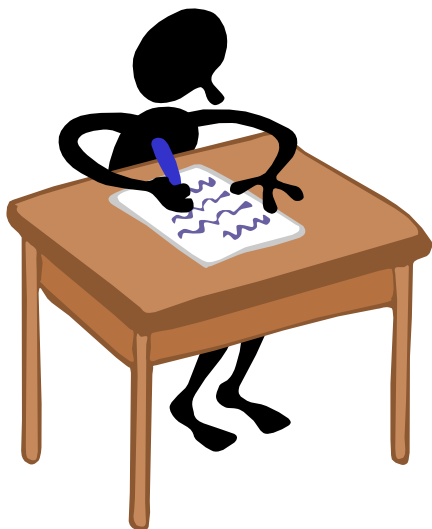
- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- www.tricare.osd.mil/tmaprivacy/Hipaa.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA Privacy representatives



HEALTH AFFAIRS



Please take your test and fill out your critique



Thanks!

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*